6712-01

This document is scheduled to be published in the Federal Register on 08/25/2023 and available online at **federalregister.gov/d/2023-18357**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Chapter I

[PSHSB: PS Docket No. 23-239; FCC 23-65 FR ID 166265]

Cybersecurity Labeling for Internet of Things

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) proposes measures to improve consumer confidence and understanding of the security of their connected devices – commonly known as Internet of Things (IoT) devices – that are woven into the fabric of their everyday lives. To provide consumers with the peace of mind that the technology being brought into their homes is reasonably secure, and to help guard against risks to communications, the Commission proposes a voluntary cybersecurity labeling program that would provide easily understood, accessible information to consumers on the relative security of an IoT device or product, and assure consumers that manufacturers of devices bearing the Commission's IoT cybersecurity label adhere to widely accepted cybersecurity standards. In this regard, the Commission's cybersecurity labeling program would help consumers compare IoT devices and make informed purchasing decisions, drive consumers toward purchasing devices with greater security, incentivize manufacturers to meet higher cybersecurity standards to meet market demand, and encourage retailers to market secure devices. The proposed IoT label would offer a trusted, government-backed symbol for devices that comply with IoT cybersecurity standards.

DATES: Comments are due on or before **[30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** and reply comments are due on or before **[45 DAYS AFTER DATE OF PUBLICATION.]** Written comments on the Paperwork Reduction Act proposed information collection requirements must be submitted by the public and other interested parties

on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: You may submit comments, identified by PS Docket No. 23-239, by any of the following methods:

- Federal Communications Commission's website: https://www.apps.fcc.gov/ecfs/. Follow the instructions for submitting comments.
- Mail: Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number. Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission. Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701. U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, DC 20554.

  Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, DA 20-304 (March 19, 2020). https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

  People with Disabilities. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530

(voice), 202-418-0432 (TTY).

FOR FURTHER INFORMATION CONTACT: Erika Olsen, Acting Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-2868, or by email to erika.olsen@fcc.gov; or James Zigouris, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0697, or by email to james.zigouris@fcc.gov. For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole Ongele, Office of Managing Director, Performance Evaluation and Records Management, 202-418-2991, or by email to PRA@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Notice of Proposed Rulemaking (NPRM), FCC 23-65, adopted August 6, 2023, and released August 10, 2023. The full text of this document is available by downloading the text from the Commission's website at: https://docs.fcc.gov/public/attachments/FCC-23-7A1.pdf. When the FCC Headquarters reopens to the public, the full text of this document will also be available for public inspection and copying during regular business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an email to FCC504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

Regulatory Flexibility Act: The Regulatory Flexibility Act of 1980, as amended (RFA), requires an agency to prepare a regulatory flexibility analysis for notice-and-comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities." The Commission seeks comment on potential rule and policy changes contained in the document, and accordingly, has prepared an IRFA. The IRFA for this document in PS Docket No. 23-239 is set forth below in this document and written

public comments are requested. Comments must be filed by the deadlines for comments on the document indicated under the **DATES** section of this document and must have a separate and distinct heading designating them as responses to the IRFA. The Commission reminds commenters to file in the appropriate docket: PS Docket No. 23-239.

Paperwork Reduction Act: This document may contain proposed modified information collection requirements. Therefore, the Commission seeks comment on potential new or revised information collections subject to the Paperwork Reduction Act of 1995. If the Commission adopts any new or revised information collection requirements, the Commission will publish a notice in the Federal Register inviting the general public and the Office of Management and Budget to comment on the information collection requirements, as required by the Paperwork Reduction Act of 1995, Public Law 104–13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), the Commission seeks specific comments on how it might further reduce the information collection burden for small business concerns with fewer than 25 employees.

Ex Parte Rules - Permit-But-Disclose. This proceeding this document initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's ex parte rules. Persons making ex parte presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral ex parte presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the ex parte presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such

data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during ex parte meetings are deemed to be written ex parte presentations and must be filed consistent with Rule 1.1206(b). In proceedings governed by Rule 1.49(f) or for which the Commission has made available a method of electronic filing, written ex parte presentations and memoranda summarizing oral ex parte presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's ex parte rules.

SYNOPSIS

I. Notice of Proposed Rulemaking in PS Docket No. 23-239

A. The Internet of Things (IoT) Landscape

1. As the world continues to become even more interconnected, malicious cyber campaigns become bolder and continue to threaten network security and privacy. Today, there are a wide range of consumer IoT products on the market that communicate over wired and wireless networks. These products are made up of various devices, and are based on many technologies, each of which presents a set of security challenges. Consumer IoT products and their component devices are susceptible to a wide range of relatively common security vulnerabilities including the continued use of default passwords, lack of regular security updates, and weak encryption and insecure authentication. Some IoT products and devices even lack any type of physical security. These vulnerabilities can be exploited by attackers to gain unauthorized access to the device or its data, launch denial of service (DoS) attacks, use the device as part of a larger botnet, or use the device as an interference generator. Compromised devices could also be forced to transmit at times and intervals selected by the attacker to interfere with other devices, either causing them to function improperly or causing a denial of service.

2. The proliferation of consumer IoT devices has opened the door to cyberattacks on

consumer products that can have serious privacy and national security consequences, ranging from theft of personal information to disruption of critical infrastructure. In just the first six months of 2021, for example, it was estimated "that more than 1.5 billion attacks have occurred against IoT devices." Cybersecurity vulnerabilities in IoT products and their devices also open a gateway to larger and more significant intrusions that may threaten national security.

B. Public and Private IoT Security Efforts

3. Significant work has already been conducted in the realm of IoT cybersecurity. There are also ongoing efforts to address IoT security labeling across both private and public sectors. In the private sector, for example, the Consumer Technology Association (CTA) convened an IoT working group tasked with supporting the advancement of the consumer IoT industry, and produced a white paper addressing the current regulatory approach to IoT. CTA has also convened with various organizations to discuss IoT baseline security capabilities. In addition, researchers at Carnegie Mellon University (CMU) conducted significant research into consumer IoT purchasing and concluded there is a need to "provide consumers with readily accessible information to help them make informed decisions about what they bring into their homes." International efforts have also advanced in the IoT labeling space.

4. In May 2021, Executive Order No. 14028 also emphasized the importance of IoT cybersecurity, noting the "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." Indeed, securing the Internet of Things forms a significant pillar in the recently-released National Cybersecurity Strategy, which noted in particular the need to advance the goals of the EO's IoT labeling efforts so that "consumers will be able to compare the cybersecurity protections offered by different IoT products, thus creating a market incentive for greater security across the entire IoT ecosystem."

5. In this respect and pursuant to that EO, in 2022 the National Institute of Standards and Technology (NIST) issued a White Paper that identified labeling criteria for cybersecurity

capabilities of IoT consumer devices, informed by existing consumer product labeling programs and input provided by diverse stakeholders, and issued a summary report about creating a cybersecurity labeling program for consumer IoT products. Additionally, NIST produced a final report, Profile of the IoT Core Baseline for Consumer IoT Products (NISTIR 8425), which identifies cybersecurity capabilities commonly needed for the consumer IoT sector, thereby providing a starting point for what consumers should consider when purchasing IoT products. From these efforts, NIST identified key elements of a labeling program, including encouraging innovation, and being practical and not burdensome, among other elements. In addition, NIST initiated a pilot IoT cybersecurity labeling program, in which it solicited contributions from stakeholders regarding how current and future-planned labeling efforts could align with the NIST recommendations. NIST describes a potential program that would educate the public on IoT cybersecurity capabilities, thereby allowing and enabling consumers in the marketplace to make informed choices about their IoT purchases.

6. The foregoing priorities and efforts, Commission experience guiding compliance assessment programs, and prior Commission action in this space (including the recent Spectrum Requirements for Internet of Things Notice of Inquiry, ET Docket No. 21-353, Notice of Inquiry, 36 FCC Rcd 14165 (2021), and efforts to address the potential for reprogrammed communications equipment to operate outside of authorized device parameters with the attendant risk of harmful interference) provide important building blocks for the Commission's analysis and inform its proposals today.

DISCUSSION

C. Establishing a Voluntary Cybersecurity Labeling Program

7. The Commission proposes to establish a voluntary cybersecurity labeling program. Given the nature of the IoT market, the Commission believes that the success of a cybersecurity labeling program will be dependent upon a willing, close partnership and collaboration between the federal government, industry, and other stakeholders. While this proposed program would be

voluntary, entities that choose to participate in the Commission's program would be required to ensure their IoT devices and products comply with the Commission's program requirements the Commission proposes to codify in its rules. As described below, the Commission proposes the use of certain baseline cybersecurity criteria and the development of product standards informed by those criteria, as well as the parameters for labeling of IoT products that conform with those standards and associated informational requirements. IoT products qualifying for the program would be authorized to use the Commission's proposed new distinctive label signifying their participation in the program and adherence to the standards set. The Commission anticipates that devices or products bearing the Commission's cybersecurity label will be valued by consumers, particularly by those who may otherwise have difficulty determining whether a product they are thinking of buying meets basic security standards. The Commission seeks comment on this proposed approach.

8. In adopting this document, the Commission concludes its consideration of IoT cybersecurity labeling issues related to the Notice of Inquiry in ET Docket No. 21-232 and EA Docket No. 21-233, and close that proceeding as to those issues. See Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program, ET Docket No. 21-232, EA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, 36 FCC Rcd 10578, para. 104 (2021) (Supply Chain NOI). That NOI raised IoT cybersecurity labeling in the specific context of the Commission's existing equipment authorization program, and although the Commission does not formally rule out building on its equipment authorization program at this stage, the Commission believes that its proposals for a voluntary labeling program building on the efforts of NIST and others as reflected in this document represent the most appropriate, and targeted, approach to IoT cybersecurity labeling that the Commission wants to explore at this time. The Commission believes that closing the Supply Chain NOI with respect to IoT cybersecurity labeling issues will focus commenters on this proceeding and spur comments that better reflect that distinct focus.

Thus, although the Commission hereby incorporates relevant comments in those dockets into this proceeding, PS Docket 23-239, the Commission also requests that, going forward, interested parties use PS Docket 23-239 for any filings. The Commission directs the Office of Engineering and Technology to provide public notice of the closed issues in ET Docket Nos. 21-232, 21-233.

D. Eligible Devices or Products

9. The Commission seeks comment on the scope of IoT devices or products for sale in the United States that should be eligible for inclusion in the Commission's labeling program. To help inform the program's scope, the Commission observes that the practical goal is to provide consumers with a clear, easily understood indicator that the IoT devices displaying the Commission's label satisfy certain baseline cybersecurity requirements and have specific cybersecurity capabilities. In assessing scope, the Commission seeks to ensure that its program would be sufficiently inclusive to be of value to consumers in this regard.

10. The Commission seek comment on whether to focus the program initially on IoT "devices" (as defined in this document) and specifically those wireless devices that intentionally emit radio frequency (RF) energy. The Commission begins by considering NIST's definition of IoT devices. NIST defines IoT devices as those devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. The Commission proposes two modifications to the NIST definition for purposes of its labeling program. First, the Commission proposes to add "Internet-connected" to its definition because, as NIST observes, a key component of IoT is the usage of standard Internet protocols for functionality, which expose IoT to related security threats and challenges caused by being Internet-connected. Second, because the Commission's relevant statutory authorities recognize the more extensive risks of harmful interference associated with devices that intentionally emit RF energy, the Commission proposes to include the premise that an IoT device must be capable of intentionally emitting RF energy. In this respect, the Commission is referring to an IoT device, with a

wireless interface, that intentionally uses RF energy to communicate or interact with the physical world. Accordingly, incorporating the Commission's modifications, the Commission proposes, for purposes of the IoT labeling program, to define an IoT device as: (1) an Internet-connected device capable of intentionally emitting RF energy that has at least one transducer (sensor or actuator) for interacting directly with the physical world, coupled with (2) at least one network interface (e.g., Wi-Fi, Bluetooth) for interfacing with the digital world. The Commission seeks comment on this proposed definition.

11. The Commission proposes to focus the scope of its program on intentional radiators that generate and emit RF energy by radiation or induction. Such devices – if exploited by a vulnerability – could be manipulated to generate and emit RF energy to cause harmful interference. While the Commission observes that any IoT device may emit RF energy (whether intentionally, incidentally, or unintentionally), in the case of incidental and unintentional radiators, the RF energy emitted because of exploitation may not be enough to be likely to cause harmful interference to radio transmissions. The Commission seeks comment on this view. Does this proposed definition unduly limit the devices that should be eligible for participation in the cybersecurity labeling program? Are there specific unintentional radiators or incidental radiators that should be included in the program, or should they be included generally? Alternatively, should the Commission consider adding these devices to the program at a later date? The Commission also seeks comment on any other ways in which the Commission's proposal might be limiting or should otherwise be expanded. For example, would the exclusion of wired-only IoT devices impact the success, usefulness and effectiveness of this labeling program and confuse consumers, rather than adequately informing them on IoT devices with appropriate network security standards?

12. To ensure that its program is able to be of greatest value to the consumer, the Commission also seeks comment on whether it should focus the cybersecurity labeling program on to IoT "products," rather than IoT devices as defined above. For such purposes the

Commission could define an IoT product consistent with the NIST definition as follows: An IoT device and any additional product components (e.g., backend, gateway, mobile app, etc.) that are necessary to use the IoT device beyond basic operational features. The Commission seeks comment on this proposed definition of an IoT product eligible for an IoT label.

13. Further, the Commission seeks comment on whether a program that addresses products (as opposed to just devices) would be more consumer friendly, as the public may find it easier to understand that the product (as a whole) they are looking to purchase meets the IoT security standards, rather than trying to parse which devices (i.e., parts of the product) meet applicable standards. Likewise, would limiting the label to devices create confusion with consumers who may not fully understand the label does not apply to the entire product? If the program only encompasses devices, should the Commission differentiate the labeling in situations where a product contains multiple devices, and some devices are labeled and some are not? If so, how could the Commission make this differentiation without causing consumer confusion? How does the Commission mitigate consumer confusion if a device label is used in a common packaging environment? The Commission seeks comment on these issues.

14. The Commission also seeks comment on whether either definition fully accounts not only for the IoT device or product itself, but also the other components that make the IoT device functional and may be vulnerable to attack. For example, there is a category of IoT devices that do not connect directly to the customer's home Wi-Fi network; instead, they connect to an intermediate communication device (i.e., Wi-Fi Gateway) which connects to the home Wi-Fi network. What are the risks and vulnerabilities inherent in the communication between these types of IoT devices or products and their environment? Are there other IoT devices or products that similarly have vulnerabilities that would be outside the scope of the Commission's proposed definition? Should such concerns be considered when adopting a definition for devices and/or products that would be eligible for the labeling program? If so, how?

15. Finally, the Commission recognizes that IoT devices and products have proliferated not

only in the non-enterprise space, but also in the workplace from office settings to field settings, from medical settings to industrial settings. As such, the Commission seeks comment on whether to focus the IoT labeling program on consumer IoT devices or products intended for consumer use or include "enterprise" devices or products intended for industrial or business use, or to otherwise tailor the scope of devices and products covered by the labeling program based on their usage. If commenters propose that the program include a broader array of devices or products beyond the non-enterprise setting, what additional considerations should the Commission take into account for these products or devices, including the relative sophistication and specific needs of the purchasers of these devices?

16. IoT Products Excluded from the Commission's Labeling Program. Pursuant to the Secure and Trusted Communications Networks Act of 2019, and the Commission's rules, the Commission's Public Safety and Homeland Security Bureau (PSHSB) publishes and regularly updates a list of communications equipment and services produced or provided by specified entities ("Covered List"), which have been determined to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons ("Covered List"). Beginning on February 6, 2023, the Commission no longer permits authorization of any applications for equipment certification of any equipment that has been identified as "covered" equipment on the Commission's Covered List. This decision did not, however, revoke any previously authorized equipment that now constitutes "covered" equipment, although it may do so in the future. In this proceeding, the Commission proposes to exclude from the labeling program any such previously authorized "covered" equipment. The Commission seeks comment on this proposal.

17. In light of this prohibition, the Commission similarly proposes to exclude from the program any communications equipment that now, or in the future, has been placed on the Covered List. The Commission proposes to exclude any IoT device that is produced by an entity identified on the Covered List as producing "covered" equipment. Furthermore, the Commission

proposes to exclude from the Commission's labeling program any device or product from a company named on the Department of Commerce's Entity List, the Department of Defense's List of Chinese Military Companies or similar lists. See, e.g., Bureau of Industry and Security, U.S. Department of Commerce, Supplement No. 4 to Part 744 – Entity List, https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file (May 19, 2023); Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Tranche 2, U.S. Department of Defense, https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF (Oct. 5, 2022).

18. The cybersecurity label has the potential to convey important information about a device or product's security. The Commission finds it could be harmful to consumers to portray such a message on devices or products made by companies that its sister agencies have identified publicly as part of their national security review. The Commission seeks comment on this proposal and on other government lists the Commission should consider. How can the Commission ensure any such proposed exclusion is implemented? Should applicants be required to include a written and signed attestation that the particular equipment for which they seek approval is not "covered" equipment (i.e., is not communications equipment that has been identified and placed on the Commission's Covered List)? Are there other products or categories of products that the Commission should explicitly exclude from the program?

E. Oversight and Management of the Proposed IoT Cybersecurity Labeling Program

19. As discussed above, the Commission believes that close partnership and collaboration between the federal government, industry, and other stakeholders is vital to ensuring the success of the proposed voluntary IoT cybersecurity labeling program. Moreover, a collaborative environment that can leverage the expertise, incentives, and authority of various constituencies in

this context would allow for the swift establishment and maturity of the program with broad industry and consumer acceptance that could adapt to a rapidly evolving threat landscape. As such, the Commission proposes a public-private partnership in the oversight and administration of this labeling program, subject to ultimate Commission supervision.

20. In seeking comment on the proposed IoT labeling program, the Commission notes that NIST identified several key elements of a potential labeling program. These include the use of certain recommended baseline product criteria (including both technical product criteria that promotes cybersecurity-related capabilities and non-technical criteria providing important product information), the use or development of requirements and/or standards that are informed by the recommended product criteria, the establishment of a conformity assessment program to assess whether particular products satisfy the developed requirements and/or standards, and the creation of labeling requirements for IoT products (a single label indicating that a product has met the baseline standard, as well as a means to access additional label information for the specific IoT product) that will aid in IoT purchasing decisions by enabling comparisons among products and providing important information about cybersecurity considerations. NIST also noted that "one size does not fit all," and that multiple solutions might be offered.

21. The Commission proposes to establish a program where the Commission would create and own a new distinctive trademark to be used in a voluntary program for IoT cybersecurity labeling and would take appropriate steps to authorize its overall use in a way that ensures the integrity of the mark and the label. The Commission also proposes to have third parties play integral roles in the management and administration of the labeling program. These entities would, for example, be authorized to conduct activities such as development of requirements or standards for consideration by the Commission, and assessment of IoT devices and products for conformity with those requirements or standards subject to supervision of the Commission. Subject to Commission oversight, third parties could evaluate and authorize the use of the Commission's trademark on an IoT device or product. In this regard, the Commission proposes

to incorporate and leverage the specialized expertise of third parties, where appropriate, into its standards, application and review procedures.

22. Oversight and Management of the Labeling Program. In NIST's White Paper on a cybersecurity labeling program for consumer IoT products, it discussed the need for management and oversight of the overall labeling program. Specifically, it contemplated that there would be one entity (the "labeling scheme owner") that would manage the labeling program, determine its structure and management, and perform oversight to ensure that the program is functioning consistently in keeping with overall objectives; further, this entity would be responsible for defining the conformity assessment requirements, developing the label and associated information, and conducting consumer outreach and education." The Commission seeks comment on the appropriate entity or entities to serve in the oversight and management of the labeling program. Should the Commission be the scheme owner to oversee as well as manage the labeling program? If the Commission takes on the role of overseeing the labeling program, should one or more third-party administrators, as detailed below, manage the tasks identified above or some portion of them? Or, should one or more third-party administrators be designated as the scheme owner(s), and if so, how should the Commission retain and exercise its oversight responsibilities?

23. Use of Third-Party Administrator(s). The Commission seeks comment on how one or more third-party administrator(s) might be utilized to manage some or all of the functions outlined above as NIST ascribed to the labeling program scheme owner, or how such an entity, or entities, might otherwise manage all or some elements of the envisioned labeling program to ensure effectiveness, efficiency, consistency, and timely implementation, subject to ultimate Commission supervision. The Commission seeks comment on the best approach for utilizing the respective levels of expertise that reside in the Commission, other federal government entities, industry, and other stakeholders. In particular, the Commission seeks comment on whether there are existing stakeholders, public or private, who are well situated to convene and develop the IoT

security standards among stakeholders as to a particular IoT device or product, or classes of IoT devices or products, to ensure the consistency and fair administration of the proposed labeling program. Further, could a third-party administrator approve, or submit to the Commission for approval, more specific standards for conformance assessment of the proposed criteria, or for otherwise evaluating program applicants? Could a third-party administrator set the requirements for testing laboratories? Should the Commission consider designating a third-party administrator or other outside entit(ies) to authorize the use of the envisioned cybersecurity label, and if so, what oversight should it exercise, for example, to ensure the integrity of the mark and label?

24. If the Commission were to utilize one or more third-party administrator(s), the Commission seeks comment on how it should select such administrator(s). What qualifications should a third-party administrator possess, and how should the Commission intake and evaluate applications? What national security considerations are relevant to such qualifications? Should a third-party administrator(s) be required to have previous experience administering an IoT product or similar conformity assessment program? Given the diversity in IoT devices and products, would it be preferable for third party administrators to have varying areas of expertise? What level of control or oversight should the Commission retain, and what level of guidance should be provided? Are there entities in this space that should be considered for this role and, if so, why? Are there benefits to utilizing multiple third-party administrators versus a single administrator? If there are multiple administrators, how could the Commission ensure standards are consistently applied across similar devices and avoid conflict among administrators? How could the Commission reconcile the functionalities of each administrator to avoid conflict? Are there other attributes or qualities that the Commission should require of an administrator? For example, should the administrator be required to be a non-profit entity? Should the administrator establish that it would be neutral and independent, with no conflicts of interest (financial or organizational) on the part of the organization or its officers, directors, employees, contractors, or significant subcontractors? Should the Commission direct PSHSB, coordinating with the

Office of the Managing Director and the Office of Engineering and Technology, to develop and implement a selection or qualifications review process?

25. Cybersecurity Labeling Authorization Bodies. The Commission seeks comment on how IoT devices or products can demonstrate compliance with the IoT security standards, once they are developed. In the context of the Commission's existing equipment authorization process, Telecommunications Certification Bodies (TCBs), which are accredited third parties recognized by the Commission, certify RF equipment based in part on testing for compliance with applicable technical RF requirements on behalf of the Commission and in accordance with the Commission's rules and standards. TCBs may then be subject to international Mutual Recognition Agreements which determine acceptance of their conformity assessment results by other countries. The Commission anticipates that it could draw from this type of program's organizational structure to assess IoT devices and products for compliance with the IoT cybersecurity standards, once they are developed. In the context of IoT labeling, instead of RF-based testing and certification, we envision that third parties with expertise in security and compliance testing, as described below, could fill this role. The Commission refers to these entities as Cybersecurity Labeling Authorization Bodies (CyberLABs) for purposes of this discussion. The Commission seeks comment on this proposal.

26. CyberLABs Accreditation or Recognition. The Commission proposes that the Commission or one of its authorized third-party administrators would evaluate, accredit, or recognize the CyberLABs based on their qualifications, resources, and procedures. If the Commission were to authorize third party administrators to evaluate, accredit or recognize these entities, what oversight would the Commission exercise over these entities or over the process? The Commission seeks to ensure that CyberLABs have the necessary expertise and resources to properly test and assess IoT devices and products compliance with the IoT security standards. To become accredited or recognized for the proposed IoT labeling program, the Commission proposes that a CyberLAB submit an application demonstrating that it meets the following

requirements:

•Qualifications: The CyberLAB has technical expertise in cybersecurity testing and conformity assessment of IoT devices and products.

•Resources: The CyberLAB has the necessary equipment, facilities, and personnel to conduct cybersecurity testing and conformity assessment of IoT devices and products.

•Procedures: The CyberLAB has documented procedures for conformity assessment.

•Continued competence: Once accredited or recognized, CyberLABs would be periodically audited and reviewed to ensure they continue to comply with the IoT security standards and testing procedures. In addition to periodic audits, the FCC or its third-party administrator would also conduct random inspections of CyberLABs to ensure that they are complying with the IoT security standards and testing and label authorization procedures. Additionally, existing standards, e.g., ISO/IEC 17025 could be leveraged for developing qualifications for a CyberLAB. See General requirements for the competence of testing and calibration laboratories, ISO/IEC 17025:2017 (Nov. 2017) (available at https://www.iso.org/standard/66912.html).

27. The Commission seeks comment on this proposed process and accompanying qualifications. Are they an appropriate fit for the Commission's objectives? Are there other options the Commission should consider? For example, could device manufacturers be allowed to perform testing and self-assessment subject to review by a third-party administrator or other entity? What additional qualifications, if any, should the Commission seek in a CyberLAB seeking to perform such as testing and conformity assessments? What additional controls might be necessary, if any, to ensure a CyberLAB remains impartial when testing and assessing IoT devices and products with relevant standards? Should the Commission take into account any national security considerations, or adopt Character Qualifications for CyberLABs? If so, what should these include? Would this accreditation or recognition process impact the Commission's existing, or future, Mutual Recognition Agreements and, if so, how might it be remedied to avoid

such impact? Should CyberLABs be located only in the United States? If the Commission should consider CyberLABs located outside the United States, what additional scrutiny, if any, should these entities be given during the Commission's accreditation process? Given the sensitive information that will be shared with CyberLABs, should accreditation or recognition include reviewing CyberLABs internal security practices? If requested by participating firms, should CyberLABs be required to provide information on their own security or internal practices to firms?

F. Development of IoT Cybersecurity Criteria and Standards

28. Applying the Baseline NIST Criteria. The Commission seeks comment on the adoption of the NIST's recommended IoT criteria as the basis for the proposed labeling program. The NIST IoT criteria are based on product-focused cybersecurity outcomes, rather than specific requirements. NIST contemplates that "the outcome-based approach allows for the flexibility required by a diverse marketplace of IoT products" and the "role of the scheme owner is critical to ensure that supporting evidence demonstrates that the product meets the expected outcomes." The NIST criteria include: (1) asset identification; (2) product configuration; (3) data protection; (4) interface access control; (5) software update; (6) cybersecurity state awareness; (7) documentation; (8) information and query reception; (9) information dissemination; and (10) product education and awareness. NIST has noted that while the first six of these criteria generally concern certain technical product criteria, the last four concern non-technical product criteria. How could NIST's IoT criteria, such as product configuration, interface access control, product education and awareness, data production, asset identification, software updates, cybersecurity state awareness, documentation, information and query reception, etc., be leveraged to inform minimum IoT security requirements and standards in a manner that is suitable for conformity assessments (e.g., for technical-related testing and non-technical verification) in appropriate circumstances, or for self-attestation in others? Are there other criteria the Commission should consider? Are there separate criteria that should be considered

for higher risk IoT devices or classes of devices?

29. Standards Development Based on NIST Criteria. The Commission recognizes that this conformity assessment program must be based on IoT security standards and testing requirements that the IoT devices and product must satisfy to be eligible to receive and use the label. The Commission proposes that the IoT security standards be developed jointly with the industry and other stakeholders. In this regard, there may be a number of expert Standards Development Organizations (SDOs), industry groups and government agencies that have both the technical expertise and other requisite experience to contribute to this task. The Commission seeks comment on whether the Commission or an outside entity is in the best position to convene these stakeholders, and to timely develop the more specific detail that would allow the consistent and replicable testing necessary to ensure the outcome based NIST IoT labeling criteria are fulfilled. Would the Federal Advisory Committee Act (FACA) limit the Commission's ability to convene these stakeholders? The Commission seeks comment on this proposal.

30. The Commission proposes that the IoT security requirements and standards would be developed and implemented through the following process:

- Collecting information: Conduct research, consult with experts, and review existing standards such as those developed and in use by international organizations.
- Establishing requirements: Informed by the new data, develop requirements that will help meet NIST core baseline criteria.
- Develop the standard: With the requirements established, the standard can be developed. This will involve creating a document that outlines the requirements in a clear and concise manner and a clear mapping between the standards and the device or product criteria.
- Reviewing and improving: Ensure that the standard is comprehensive, clear, and suitable for lab testing.
- Implementation: Conduct training, testing, and monitoring to ensure that the

requirements are satisfied.

31. The Commission seeks comment on the scope of this work and on this proposed process. What additional factors should be included or otherwise factored into this process? How can the Commission ensure that the views of small, women- and minority-owned businesses, including small IoT manufacturers, are considered in this process? Considering the amount of work that the industry, NIST, and international community have already completed in this area, how could this work be leveraged to promote the swift development of standards for IoT cybersecurity labeling? How long might this work take to complete? The Commission seeks comment on the shortest but most thorough path to accomplishing this work and the minimum amount of time it should take to develop the standards. The Commission recognizes there are other IoT security standards already available and seek comments on whether and why the Commission should consider their adoption. Are there standards for particular IoT devices or classes of IoT devices that are already sufficiently mature such that they could be readily – or more quickly – adopted? Should the program start with those devices or products?

32. The Commission recognizes that while the IoT cybersecurity label would not constitute a guarantee that the participating IoT product can withstand every single cyberattack, it should provide meaningful assurance to consumers that the IoT devices and products that display the label satisfy certain minimum cybersecurity standards and have specific cyber capabilities that demonstrably reduce relevant vulnerabilities appropriate to the class of device. As such, while participation in the IoT labeling program would be voluntary, the Commission proposes to require those who choose to participate to adhere to the specific standards described above, and as recognized by the Commission.

33. The Commission observes that in other contexts, it periodically incorporates by reference various standards established by standards-setting bodies including, but not limited to, the American National Standards Institute (ANSI), Accredited Standards Committee C63 (ANSC C63), and the International Organization for Standardization; and the International

Electrotechnical Commission. As the Commission has noted, use of industry-based standards in this context is intended to ensure the integrity of the measurement data associated with an equipment authorization. The Commission recognizes that, in addressing cybersecurity standards, timely adoption and speed are a prime benefit of a multi-stakeholder, industry-led approach, which militate in favor of a more streamlined process than the full Commission-level review described above. Accordingly, the Commission proposes if standards are developed by outside bod(ies), that they submit the IoT security standards for acceptance by the Commission prior to utilization for testing and other conformity evaluation. In this regard, the Commission proposes to direct PSHSB to place the standards on Public Notice for comment in accordance with the rulemaking requirements of the Administrative Procedure Act and, subsequent to reviewing any comments received, accept the standards as proposed or with amendments as warranted by the record. Is this sufficient, or do commenters believe a Commission-level rulemaking is needed? Alternatively, could an outside body adopt the standards and attest their conformity with the broader NIST criteria in a manner acceptable to the Commission, without the need for further action by the Commission? What other streamlined processes might be appropriate for prompt review and validation of IoT security standards?

34. Conformity Assessments. The Commission seeks comment on the process for assessing conformity of consumer IoT products and devices under the Commission's IoT labeling program. While the Commission expects that third-party assessment (testing and other required assessment via CyberLAB, as discussed above) would provide an avenue for conformity assessment, the Commission proposes that other approaches also be considered. For example, NIST describes how different IoT conformity assessment activities could be leveraged to demonstrate that consumer IoT devices conform to technical requirements, either exclusively or in combination. In addition to third-party testing, assessment activities could also include the supplier's declaration of conformity/self-attestation of the consumer IoT device where a statement is issued based on a comprehensive review that an IoT device or product comply with

the IoT security standards. While the Commission's equipment authorization program has evolved over the years, as currently administered the program includes two procedures for equipment authorizations – certification and Supplier's Declaration of Conformity (SDoC). Relevant technical RF-based standards listed in section 2.910 of the Commission's rules are incorporated by reference in Part 2. The rules specify the obligations of the "responsible party" (e.g., the manufacturer or importer), including warranting that each unit of equipment marketed under the grant of certification or SDoC is materially identical to the unit that was tested or measured. The Commission seeks comment on the extent to which any of these same procedures may be appropriate for the IoT labeling program. Are there other alternative procedures that are more suitable for the IoT labeling program context?

35. Third-Party Compliance Testing and Assessment. The Commission proposes that conformity assessments for IoT devices and products be based on compliance assessment (any testing and other requisite assessment) that includes supporting documentation and data submitted by the manufacturer or importer of the IoT device or product in question to a third-party such as a CyberLAB, and that the third party administrator could authorize the use of the IoT security label only for devices that meet the established IoT security standards. Should all IoT devices or products be required to pursue third party compliance assessment, or are there classes of IoT devices or products that should allow for self-attestation?

G. Administering the IoT Labeling Program

36. Commission to Obtain Trademark. The Commission proposes that the Commission utilize a certification mark to identify those products that meet the Commission's IoT labeling requirements. A certification mark is a type of trademark that is used to show consumers that particular goods and/or services, or their providers, have met certain requirements. Specifically, the mark indicates that: (1) the owner of the mark controls who may use the mark; (2) the owner of the mark has determined that the user complies with a specific standard described by the owner of the mark; and (3) the owner of the mark does not itself produce the goods or services

covered by the mark. The Commission has applied for a mark with the United States Patent and Trademark Office (USPTO), and as the owner of the mark, should this proposal be adopted, will ensure that the IoT products and devices bearing the mark meet FCC-approved cybersecurity labeling program requirements. The Commission also seeks comment on whether the Commission should permit outside entities to authorize use of the mark where the terms of the program are met and what measures are necessary to ensure that the Commission is effectively controlling the use of the mark for purposes of trademark law.

37. Commission IoT Label. The Commission proposes to implement a single binary label with layering. Under a binary label construct, products or devices will either qualify to carry the label or not qualify (i.e., not be able to carry the label) and "layers" of the label would include the Commission's IoT mark representing that the product or device has met the Commission's baseline consumer IoT cybersecurity standards and a scannable code (e.g., QR code) directing the consumer to more detailed information of the particular IoT product.

38. The Commission seeks comment on where authorized program participants should affix the security IoT label. If the Commission's program addresses devices (rather than products), should it be affixed on each IoT device or on the product packaging? Should equipment that includes a user display screen be permitted to display the label on the user display screen rather than on the device itself? Should there be limitations or prescriptions on how companies and third-party resellers can use the mark in advertising or sales displays, products or websites? The Commission also seeks comment on other approaches with regard to what the label should display and where the label should be placed.

39. Layered Information. The Commission seeks comment on the use of a QR code or URL to enable consumers to access more detailed information about the device or product, including specific security information, such as the device manufacturers' level of support, software update history, privacy policy, and similar information. To provide consumers with uniform information and minimize the potential for consumer confusion, the Commission proposes that

there be a single IoT device or product registry associated with the Commission's IoT cybersecurity labeling program, and that any QR code or URL included with the FCC IoT mark provide a link to the IoT product's specific webpage within this IoT registry. The Commission proposes to prohibit any additional QR codes or URLs be placed in connection with the Commission's IoT mark. The Commission believes that this would help ensure the integrity of the Commission's IoT label. If third parties are authorized by the Commission to grant use of the cybersecurity IoT label, should the Commission also permit them to generate and specify the QR code and the URL that can be placed next to the FCC IoT mark and require them to prevent the program participants from affixing other QR codes or URLs next to the FCC mark? Should the use of the IoT mark be prohibited without the associated QR code or URL? What information must a company include if they reference the IoT mark in product listings or descriptions? What alternative approaches should the Commission consider?

40. QR Code. The Commission proposes that the FCC IoT label include a QR code that contains consumer-friendly information that is available without Internet connection in addition to a URL to the device's or product's registry page, which is discussed below. (While the Commission thinks the use of a QR code is appropriate in conjunction with the layered labeling approach it is proposing here, the Commission acknowledges that it previously rejected its use in other contexts, such as the required labeling under its equipment authorization rules. The Commission is not proposing to revisit those decisions in the context of this proceeding. Similarly, the Commission intends its proposals to operate distinct and separate from the provisions for the electronic labeling of radiofrequency devices contained in its equipment authorization rules (47 CFR 2.935), and seeks comment on whether it needs to adopt or modify its rules accordingly.) In order to prevent consumer confusion and allow for easy comparison among devices or products, the Commission also proposes that the information contained within the QR code for each certified device or product be uniform and include information that is helpful to non-expert, home users of IoT devices and products. In this way, the label would be

able to impact consumer purchasing decisions, which are oftentimes made under time pressure while the consumer is at the store choosing between products. The Commission proposes the QR code include a description of the device's security (e.g., easy to understand explanation of what security standards the device meets, and how these standards protect the consumer). The Commission also proposes the QR code include a statement that while the label indicates the device or product meets certain cyber security criteria that reduce risk, it does not eliminate risk entirely and the label does not imply product endorsement by the label program and that the consumer is encouraged to visit the product registry linked by the URL provided therein to get the most up-to-date security and other information related to the IoT device or product. The Commission seeks comment on this proposal and what additional or other information should be embedded in the QR code to be of benefit to consumers.

41. Given the static nature of the information stored in the QR code, the Commission urges commenters to consider the types of information that would be appropriate for consumer decision-making without needing to have the information stored in the QR code updated. Alternatively, the QR code could merely provide a link to the IoT registry page for the device or product in question, discussed below.

42. The Commission proposes to require that the manufacturer disclose the guaranteed minimum support period for an IoT device or product, during which the manufacturer commits to identify and patch security vulnerabilities in the product. See NIST, Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products, at 10 (Feb. 4, 2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf. While the Commission recognizes the length of such a support period is at the discretion of the manufacturer, and may even be zero, the Commission seeks comment on the benefits and drawbacks of requiring a manufacturer to disclose, via the label or associated registry entry, the length of time that an IoT device or product would be supported, and the level of support provided. Should they also be required to disclose whether all or only critical patches will be supported, the regularity with

which such patches are made available, whether they are automatically deployed, or what additional steps a consumer may need to take to remain secure when support ends? Should the Commission require the manufacturer to provide notice when that support ends? How can the Commission ensure this information is meaningful to consumers? The Commission seeks comment on these options and any alternatives to help provide consumers with necessary, accurate, and timely information.

43. IoT Registry. The Commission proposes the use of an IoT registry where the public may access a catalog of devices or products that are approved pursuant to the Commission's IoT labeling program. This IoT registry would be accessible via the Internet and serve as a one-stop reference for the public to understand which products in the market bear the IoT label (e.g., consumers could check the registry before they shop). The IoT registry could contain IoT security-related information that is sortable and searchable by manufacturer or brand, device or product vendor, device or product name, model number, firmware/software build version, and other identifying variables, such as a unique asset identification number. The Commission seeks comment on this approach. Are there any similar product registries that have already been established or that are being initiated, and that might be leveraged for these purposes? Should the Commission consider selecting and overseeing a third-party IoT registry administrator, and if so, how could such an administrator be funded? Should there be more than one administrator or more than one registry, and if so, how should the Commission ensure that accurate, up to date, and complete information is contained in each of them? Should it be the same third-party administrator contemplated to manage the other aspects of the labeling program as described herein?

44. The QR code and/or the URL associated with the IoT label would include a link to the IoT registry, which would provide detailed information on the IoT product through the product's webpage within the IoT registry. The Commission seeks comment on what information should be included within the IoT registry and associated with the QR codes. If the URL is the sole

piece of information associated with the QR code, how should registry information be presented or organized to ensure consumer-friendliness?

45. The Commission proposes that, among other information, the IoT registry might provide the following information for each approved device (or product): 1) how to operate the device securely (e.g., basic cyber hygiene to include changing default passwords) and, if applicable, what level of security the device or product has achieved; 2) whether the product's security settings are protected against unauthorized changes, including disabling its security; 3) where the device was manufactured; and 4) when the registry information for the device was last updated. What other information should be included? Would the information included in the CMU IoT Security and Privacy Label (CMU Label) be an appropriate model for each IoT product's listing provided within the IoT registry? CMU Labels are divided into three major sections: 1) security mechanisms, 2) data practices, and 3) more information, with various data fields under these sections (e.g., security updates, access control, sensor type, privacy policy, manufacturer contact information, and platform compatibility). CMU Labels often link to external sites, such as manufacturers' websites, to provide more detailed information. Would linking to external websites, over which the Commission would have no oversight or control, be appropriate for the Commission's IoT labeling program and the IoT registry? How could the Commission ensure the content of the information provided in the external links is accurate and up-to-date? Are there additional exemplary labels that the Commission should consider? What other additional details should be disclosed to inform consumers of cybersecurity risks underlying the IoT product? What details can potentially be omitted? How can the Commission otherwise ensure the information provided in the IoT registry is meaningful and understandable by consumers?

46. The Commission further asks whether such IoT registry might also be used by retailers to assist them with choosing products that carry the IoT label for sale in their stores and whether retailers may use the registry to confirm that the products that they market legitimately bear the FCC's IoT label. If so, should the registry maintain different sets of information for general

consumers and retailers? What additional information would retailers want to see but is not relevant to general consumers?

47. Updating Information. The Commission seeks comment on how to ensure consumers are not misled by the meaning of the IoT label and can obtain up-to-date information about their device or product. Unlike other labeling programs, such as the Commission's Broadband Consumer Label, or the ENERGY STAR label, the Commission's labeling program addresses cybersecurity risk, which is constantly changing and requires constant updating. For example, if a new vulnerability is discovered, the product would remain unsecure until that newly discovered vulnerability is patched. The Commission proposes that consumers be made aware of any vulnerabilities or updated product information through the IoT registry. That way, once the product's webpage within the IoT product registry is updated to indicate that the authorization to use the mark is outdated, and/or the device is no longer maintained/updated, the consumer can understand this information by accessing the webpage using the QR code and/or the URL provided next to the FCC IoT label. Should the Commission impose a duty on manufacturers or importers of the IoT devices and products to notify the IoT registry operator when they become aware of an unpatched vulnerability that poses security risks to their IoT devices and products? Are there other events that should trigger IoT product manufacturers or importers to notify the registry operator that their IoT registry device or product page should be updated?

48. The Commission seeks comment on these proposals, and on any other ways to ensure consumers have up-to-date information regarding IoT devices or products labeled under the program, as well as have an understanding that the FCC cybersecurity label is not a guarantee against all cybersecurity threats. What additional information might be warranted to help minimize the potential for customer confusion?

49. Application/Renewal. The Commission proposes that IoT label applicants file for renewal each year, together with supporting evidence that the products still meet the FCC's IoT requirements, as tested and administered by the CyberLABs or as self-attested. In this regard,

the Commission seeks to ensure consumers have up-to-date information regarding the participating device or product, and to address end-of-life issues for devices previously approved, but that no longer warrant continued authorization to use the label. Should the label include the specific date, or the year, the label was awarded to help notify consumers how fresh the authorization is? Should the FCC IoT labels on the device or product have an expiration date? How does the Commission ensure consumers are aware of when a device with an FCC IoT label is no longer maintained and/or updated by manufacturers, and may no longer meet up-to-date cybersecurity requirements?

50. The Commission seeks comment on this proposal to employ a renewal process. Should the Commission consider other timeframes on a shorter or longer basis? Should there be an event in the product's life-cycle or a security event that should trigger the applicant to file for an early renewal? When would such an event trigger early renewal, versus filing updated information with the program administrator and updating the IoT registry? Similarly, are there incidents or developments that might warrant the removal of the IoT cybersecurity label, and what might those circumstances be? After the IoT device or product is authorized for the first time, what supporting documents should the program participants provide to validate and renew their authorization to use the label? Must it be retested annually? How should the IoT registry reflect that an authorization to use the label is out of date?

51. The Commission also seeks comment on the interplay between the proposed IoT cybersecurity labeling program and its current equipment authorization rules. Given that the review process for the proposed program will likely not be administered in the same manner, and by the same entities, as are involved in its equipment authorization program, the Commission proposes that they generally operate in a distinct manner. However, given that equipment subject to the requirements of the Commission's equipment authorization rules must satisfy those rules before they can be manufactured and sold in the United States, the Commission proposes that approval be granted under the cybersecurity labeling program only after any applicable

requirements of the equipment authorization rules have been satisfied for the relevant device or product. The Commission seeks comment on these proposals and on any other ways in which it should address the potential interplay between the proposed IoT cybersecurity labeling program and its current equipment authorization rules.

52. Costs. The Commission permits TCBs to establish and assess fees for processing equipment authorization applications and conducting other Commission-required tasks. The Commission anticipates that similarly situated third parties in this program may wish to charge for their services and seek comment on whether there is any oversight the Commission needs to exercise over such charges. Further, the Commission proposes, that when a proposed grant of labeling authority is submitted to the Commission for action it should be accompanied by an application fee pursuant to its authority under section 8 of the Communications Act. The Commission proposes to follow the fee calculation methodology adopted by the Commission in the 2020 Application Fee Report and Order. The Commission seeks comment on this proposal and any changes or modifications the Commission should consider here.

53. Investigation, Disqualification, and Enforcement. Ensuring that the label remains a trusted and valuable resource to purchasers requires that the integrity of the devices and products bearing the label is maintained. As such, the Commission seeks comment on how to enforce the labeling program requirements. To the extent that non-Commission entities are better situated to perform, and receive approval to perform, certain functions, should they also be required to conduct a certain number of random audits of the certified IoT devices and products to confirm that they are in compliance? Are there types of market surveillance that should be conducted, and by whom? Should the Commission allow consumer or third-party complaints? Should the Commission or other entities accept and process such complaints? What should the Commission's role be in audit and oversight? For any non-compliance, the Commission could rely on a combination of enforcement procedures such as administrative remedies under the Communications Act (e.g., show cause orders, revocation proceedings, forfeitures, consent

decrees, cease and desist orders, and penalties) or civil litigation for breach of contract or trademark infringement, in which the Department of Justice (DOJ) would participate. As noted above, the Commission also seeks comment on what, if any, additional measures are necessary to ensure that the Commission is effectively controlling use of the certification mark for purposes of trademark law. What enforcement measures would be appropriate for firms that falsely put the IoT certification mark or label on their products? How would it be enforced if firms are outside of the United States? In the more contractual context of the ENERGY STAR program, EPA has set out certain Disqualification Procedures that it would apply if a product fails third-party verification testing, or if it fails subsequent Department of Energy (DOE) appliance testing or in the event of product nonconformity. In particular, this process gives the ENERGY STAR Partner notice and an opportunity to dispute the assessment with EPA before a formal disqualification decision is made. The Disqualification Procedures specify certain steps that ENERGY STAR Partners must take in the event of a disqualification (e.g., removing references to ENERGY STAR in the product labeling, marketing, etc.). Should the Commission adopt a similar disqualification procedure under its rules? What enforcement measures would be appropriate in addition to revoking authorization to use the IoT label? What procedures or consequences should apply where a device or product was certified under one set of standards but is not capable of meeting a new or updated standard adopted later? How should the participants address the products that have the IoT security labels affixed to their products when their products become non-compliant? If an applicant is denied authority to use the Commission's IoT label, should they be able to appeal that decision? The Commission also seeks comment on any recordkeeping and audit requirements for compliance review purposes.

54. Conversely, where a program participant has received authorization to utilize the Commission's IoT Label and has appropriately maintained the device's security measures, does this represent an indicium of reasonableness that might serve as a defense or safe harbor against liability for damages resulting from a cyber incident, e.g., data breach, denial of service, malware? While the Commission

clarifies that it does not intend at this time for the labeling program in and of itself to preempt otherwise existing law, are there other affirmative measures that the Commission should consider adopting that should be afforded to devices that have achieved and maintained a Commission IoT security label?

55. Consumer Education. The Commission expects that the success of this program will rely upon a robust education campaign with shared responsibilities among the scheme owner, manufacturers, retailers, industry, and non-profit security groups to promote label recognition, brand trust, and transparency of what the Commission's IoT cybersecurity label means. The Commission seeks comment on whether the education campaign used should be comprised of the consumer education materials recommended by NIST, which include providing consumers online access to information addressing:

- Intent and Scope: What the label does and does not mean, including addressing potential misinterpretations (e.g., stating that meeting the label security criteria reduces risk but does not eliminate it entirely, and that labeled products are not necessary more secure than unlabeled products); and a statement that the label does not imply product endorsement by the Commission;
- Product Criteria: The cybersecurity properties that must be met for a device to have the Commission label and how and why these properties were selected; including information on how the criteria address security risks both to the consumer and to others for common intended uses of the products;
- A glossary of applicable technical terms written in plain English;
- General information about conformity assessment and how cybersecurity properties are evaluated;
- Declaration of Conformity: The device's specific declaration of conformity to the IoT security standards, including the date the label was last awarded;
- Scope: The kinds of devices eligible for the label and an easy way for consumers to identify labeled devices;

- Changing applicability: The current state of device labeling as new cybersecurity threats and vulnerabilities emerge;
- Security considerations for end-of-life IoT devices and implications for functionality if the device is no longer connected;
- Expectations for consumers: The responsibility consumers share in securing the device software and how their actions (or inactions) can impact the device's software cybersecurity; and
- Contact information for the labeling program and information on how consumers can lodge a complaint regarding a product label.

56. The Commission seeks comment on anticipated costs of such a consumer education campaign particularly with regard to upfront costs that will be incurred to start the program. The Commission also seeks comment on mechanisms for conducting the outreach consistent with the constraints on federal outreach and the possibility of public or private partnerships that may facilitate a consumer education campaign.

57. Integrity of the National Government-based IoT Cybersecurity Label. The Commission seeks comment on ways to avoid consumer confusion between the government-based IoT cybersecurity label and existing and future IoT cybersecurity labeling schemes such as UL and IoT Security Trust Mark. What features and assurances can the Commission's label provide to improve customer awareness of the security of a given IoT device? Alternatively, should the FCC label act as an aggregator for other labeling programs ensuring that these programs meet the IoT security standards in addition to any wider or sector specific security needs the scheme owners feel necessary. What about other labeling programs in other countries? How should the Commission coordinate and engage with other international bodies maintaining labeling programs to develop recognition of the Commission's IoT Label, and where appropriate, mutual recognition of those international labels? The Commission's proposal seeks to implement this program for devices or products for sale in the United States. What steps, if any, should the

Commission take to ensure the FCC label is not mistaken for compliance with IoT security or RF-emission standards in other countries?

58. Accessibility. The Commission emphasizes its continued commitment to ensuring that the labeling program is accessible and usable by individuals with disabilities. With respect to the Commission's Broadband Consumer Label, in 2022, the Commission noted that the Consumer Advisory Committee (CAC) determined that participating providers can best ensure accessibility to printed and online information by relying on well-established legal requirements included in the Americans with Disabilities Act and by following the guidance developed by the Web Accessibility Initiative. The Commission seeks comment on whether relying on these guidelines provides the best likelihood of ensuring that consumers with disabilities will be able to access necessary information about their IoT devices or products. The Commission seeks comment on how best to ensure that any adopted IoT cybersecurity label is accessible to persons with disabilities.

Legal Authority

59. The Commission tentatively concludes that it has authority to adopt the proposed IoT labeling program. In particular, section 302(a) of the Communications Act authorizes the FCC "consistent with the public interest, convenience, and necessity, [to] make reasonable regulations (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications; . . ." While this program would be voluntary, entities that elect to participate would need to do so in accordance with the regulations the Commission adopts in this proceeding, including but not limited to the IoT security standards, compliance requirements, and the labeling program's operating framework. The Commission tentatively concludes that the standards the Commission proposes to apply when administering the proposed labeling program fall within the scope of "reasonable regulations… governing the interference potential of devices…." The Commission seeks comment on this

reasoning.

60. The Commission has exercised authority in other contexts to secure both software and firmware to prevent unauthorized modification that would compromise a device or the data it transmits. For example, in adopting technical rules for the Citizens Broadband Radio Service (CBRS), the Commission required end user devices to "contain security features sufficient to protect against modification of software and firmware by any unauthorized parties" and required that such devices "be able to protect the communication data that are exchanged between these elements." The Commission adopted a further obligation for identified security vulnerabilities to be resolved on a going-forward basis, and encouraged industry to develop best practices for end-to-end security that can be validated through the certification process. By way of further example, in the 5 GHz band, the Commission, noting the potential for reprogramming of unlicensed national information infrastructure (U-NII) devices to operate outside of authorized device parameters, similarly adopted security measures requiring manufacturers to prevent software changes that would result in this outcome. Declining to mandate specific software security measures, the Commission required manufacturers instead to document their methods. In addition, the Commission's rules require security protocols and procedures to ensure the integrity of transmission related between and among white space devices and databases.

61. The Commission's proposed labeling program rules are intended to ensure that IoT devices have implemented certain minimum cybersecurity protocols to prevent their being hacked by bad actors who could cause the devices to cause harmful interference to radio communications. As noted above, in the 5 GHz context, the Commission identified concerns about security vulnerabilities that could, if exploited, lead equipment to operate outside established parameters, with the associated risk that doing so could cause harmful interference. As also noted above, interference issues also could arise if security vulnerabilities were exploited to use a device as an interference generator, or to transmit at times and intervals selected by the attacker to interfere with other devices. The Commission anticipates that this could be a more

pervasive risk, and the Commission seeks comment on that predictive judgment. Furthermore, under the Act, the Commission's other obligations in this regard can encompass not only the prevention of interference to other devices, but the need to mitigate against the risk of interference to covered equipment. In this regard, and in considering the potential need to encompass not only devices but, ultimately, products in order to adequately secure the IoT ecosystem and empower consumer choices, the Commission believes such an approach is reasonable under sections 333 and 302(a) of the Act.

62. In particular, the Commission also seeks comment on the authorities that would support including additional IoT products and devices within the proposed IoT labeling Program. For example, section 302(a)(2) of the Act provides the Commission with the authority to adopt reasonable regulations "establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy." Does this authority support reasonable regulations that may include the regulations proposed herein? Section 333 states: "No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government." Does this authority, possibly coupled with other provisions, provide a basis for the Commission's proposed action? Is the Commission's proposal necessary or reasonably ancillary to the execution of its implementation of any or all of these statutory responsibilities?

63. Is it reasonable for the Commission's labeling program to not only guard against the risk that covered devices and products cause harmful interference, but also to guard against other risks, including the risk of interference to those covered devices and products consistent with policy goals underlying sections 302(a)(2) and 333 of the Act? For example, the Commission tentatively concludes that its authority to adopt "reasonable regulations" to guard against harmful interference under section 302 of the Act authorizes a labeling program that applies a set of criteria or standards that address not only risks of harmful interference *from* the products or

devices subject to labeling but also other harms, such as the risk of harmful interference *to* such products or devices—particularly where the relevant criteria or standards were designed or intended to be applied as a package or collectively.

64. The Commission also tentatively concludes that its authority under section 302(a)(1) of the Act to adopt reasonable regulations consistent with the public interest to guard against interference provides the Commission flexibility to tailor the proposed labeling program in other ways. For example, the Commission believes that, in adopting reasonable regulations consistent with the public interest under section 302, the Commission has authority to exclude equipment from the Covered List from participating in the voluntary labeling program, consistent with the objectives of sections 2(a) and (d) of the Secure and Trusted Communications Networks Act of 2019. The Commission further tentatively concludes that its section 302 authority likewise enables it to rely on third parties in carrying out the implementation details of the proposed labeling program. In particular, section 302(e) of the Act authorizes the Commission to delegate equipment testing and certification to private laboratories, and the Commission notes in that regard that it already has relied in part on third parties in carrying out its equipment authorization rules. The Commission also seeks comment on whether its authority to adopt reasonable regulations in the public interest to carry out the objectives of section 302 authorizes the Commission to rely on a third party IoT registry administrator as well as rely on third parties to perform some of the functions described above.

65. The Commission also seeks comment on whether section 301 of the Act also provides the Commission with authority to include in its labeling program IoT products and devices that might receive harmful interference from an unauthorized cyber event. The Commission also recognizes, for example, that cyberattacks utilizing IoT vulnerabilities may not only give rise to harmful interference concerns, but can also effectuate physical threats to the world around us – degrading wireless networks, for example, changing service settings on smart appliances, or – more catastrophically – shutting down an industrial control system. Are there additional

authorities that support the inclusion of additional IoT products and devices that do not emit RF externally for purposes of communications, such as unintentional or incidental radiators, or wired-only IoT?

66. The Commission seeks comment broadly its legal authority under the Communications Act, or any other source, to implement the proposed voluntary IoT labeling program, including its authority pursuant to Titles II and III as well as its authority under section 4(i) of the Communications Act, as amended, to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions" which includes "the purpose of promoting safety of life and property."

67. The Commission further seeks comment on how it may utilize enforcement authorities under the Act, including the potential imposition of penalties under section 503 and cease and desist orders under section 312 for those entities that voluntarily participate in the labeling program, but fail to continue to comply with the Commission's regulations. Would participants in the labeling program already be holders of authorizations within the meaning of section 503(b)(5) of the Act, or are there steps the Commission should take to structure the labeling program so that participation would itself satisfy that provision? Are there any additional avenues for enforcement or oversight of the program's participants or of a third-party security certifying body? What trademark remedies are available to the Commission? Are there other agencies that might contribute to program enforcement?

Promoting Digital Equity

68. The Commission, as part of its continuing effort to advance digital equity for all,[84] including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations[85] and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, the Commission seeks comment on how its proposals may promote or inhibit

advances in diversity, equity, inclusion, and accessibility, as well as the scope of the Commission's relevant legal authority.

APPENDIX A

69. Within the scope of a consumer IoT product, the following baseline product criteria are recommended by NIST to define the cybersecurity outcomes expected of IoT products and IoT product developers as part of a consumer IoT product labeling program. Most criteria concern the IoT product directly and are expected to be satisfied by software and/or hardware means implemented in the IoT product. Some criteria apply to the IoT product developer rather than to the IoT product directly. These criteria are expected to be satisfied through actions and supported by assertions and evidence from the developer rather than from the IoT product itself.

70. **Product criteria are recommended to apply to the IoT product overall, as well as to each individual IoT product component (e.g., IoT device, backend, companion app), as appropriate.** (Given the nature of consumer IoT product, it is expected that all IoT products should satisfy all technical product criteria since they will, in most cases, be finished products intended for direct plug-and-play use. Individual IoT product components, though, may be more likely to not require certain criteria (e.g., based on lack of applicability). A scheme owner has the flexibility to adapt the product criteria and determine appropriate supporting evidence. Though NIST recommends that all criteria apply to every IoT product, some components may not be able or need to support all criteria. That might be the case due to product risk considerations, product development (e.g., cybersecurity tasks delegated via contracts and supply chain), nature of the components to form the product (e.g., backends may be highly distributed), or limitations of IoT components (e.g., devices may be constrained, companion software apps may have limited access and functionality).

Asset Identification: The IoT product is uniquely identifiable and inventories all of the IoT product's components.

- The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).
- The IoT product uniquely identifies each IoT product component and maintains an up-to- date inventory of connected product components.

Cybersecurity utility: The ability to identify IoT products and their components is necessary to support asset management for updates, data protection, and digital forensics capabilities for incident response.

Product Configuration: The configuration of the IoT product is changeable, there is the ability to restore a secure default setting, and any and all changes can only be performed by authorized individuals, services, and other IoT product components.

- The customer can change the configuration settings of the IoT product via one or more IoT product components.
- The IoT product applies configuration settings to applicable IoT components.

Cybersecurity utility: The ability to change aspects of how the IoT product functions can help customers tailor the IoT product's functionality to their needs and goals. Customers can configure their IoT products to avoid specific threats and risk they know about based on their risk appetite.

Data Protection: The IoT product and its components protect data stored (across all IoT product components) and transmitted (both between IoT product components and outside the IoT product) from unauthorized access, disclosure, and modification.

- Each IoT product component protects data it stores via secure means, including the ability to delete or render inaccessible data stored that is either collected from or about the customer, home, family, etc.
- When data is sent between IoT product components or outside the product, protections are used for the data transmission.

Cybersecurity utility: Maintaining confidentiality, integrity, and availability of data is

foundational to cybersecurity for IoT products. Customers will expect that data is protected and that protection of data helps to ensure safe and intended functionality of the IoT product.

Interface Access Control: The IoT product and its components restrict logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.

- Each IoT product component controls access (to and from) all interfaces (e.g., local interfaces, network interfaces, protocols, and services) in order to limit access to only authorized entities. At a minimum, the IoT product and its components shall:
  a. Use and have access only to interfaces necessary for the IoT product's operation. All other channels and access to channels are removed or secured.
  b. For all interfaces necessary for the IoT product's use, access control measures are in place (e.g., unique password-based multifactor authentication).
  c. For all interfaces, access and modification privileges are limited.
- The IoT product executes means via some, but not necessarily all, components to protect and maintain interface access control. **At a minimum, the IoT product shall:**
  a. Validate that data sent to other product components matches specified definitions of format and content.
  b. Prevent unauthorized transmissions or access to other product components.
  c. Maintain appropriate access control during initial connection (i.e., on-boarding) and when reestablishing connectivity after disconnection or outage.

Cybersecurity utility: Inventorying and controlling access to all internal and external interfaces to the IoT product will help preserve the confidentiality, integrity, and availability of the IoT product, its components, and data by helping prevent unauthorized access and modification.

Software Update: The software of all IoT product components can be updated by authorized individuals, services, and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.

- Each IoT product component can receive, verify, and apply verified software updates.
- The IoT product implements measures to keep software on IoT product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via the IoT product).

Cybersecurity utility: Software may have vulnerabilities discovered after the IoT product has been deployed; software update capabilities can ensure secure delivery of security patches.

Cybersecurity State Awareness: The IoT product supports detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.

- The IoT product captures and records information about the state of IoT components that can be used to detect cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.

Cybersecurity utility: Protection of data and ensuring proper functionality can be supported by the ability to alert the customer when the device starts operating in unexpected ways, which could mean that unauthorized access is being attempted, malware has been loaded, botnets have been created, device software errors have happened, or other types of actions have occurred that was not initiated by the IoT product user or intended by the developer.

Documentation: The IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.

- Throughout the development lifecycle, the IoT product developer creates or gathers and stores information relevant to the cybersecurity of the IoT product and its product components, **including**:

a. Assumptions made during the development process and other expectations related to the IoT product, including:
    i. Expected customers and use cases.
    ii. Physical use, including security of the location of the IoT product and its product components (e.g., a camera for use inside the home that has an off switch on the device vs. a security camera for use outside the home that does not have an off switch on the device), and characteristics.
    iii. Network access and requirements (e.g., bandwidth requirements).
    iv. Data created and handled by the IoT product.
    v. Any expected data inputs and outputs (including error codes, frequency, type/form, range of acceptable values, etc.).
    vi. The IoT product developer's assumed cybersecurity requirements for the IoT product.
    vii. Any laws and regulations with which the IoT product and related support activities comply.
    viii. Expected lifespan and anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and length and terms of support.
b. All IoT components, including but not limited to the IoT device, that are part of the IoT product.
c. How the baseline product criteria are met by the IoT product across its product components, including which baseline product criteria are not met by IoT product components and why (e.g., the capability is not needed based on risk assessment).
d. Product design and support considerations related to the IoT product, *for example*:
    i. All hardware and software components, from all sources (e.g., open source, propriety third-party, internally developed) used to create the IoT product (i.e., used to create each product component).

ii. IoT platform used in the development and operation of the IoT product, its product components, including related documentation.

iii. Protection of software and hardware elements implemented to create the IoT product and its product components (e.g., secure boot, hardware root of trust, and secure enclave).

iv. Consideration of the known risks related to the IoT product and known potential misuses.

v. Secure software development and supply chain practices used.

vi. Accreditation, certification, and/or evaluation results for cybersecurity-related practices.

vii. The ease of installation and maintenance of the IoT product by a customer (i.e., the usability of the product).

e. Maintenance requirements for the IoT product, *for example*:

i. Cybersecurity maintenance expectations and associated instructions or procedures (e.g., vulnerability/patch management plan).

ii. How the IoT product developer identifies authorized supporting parties who can perform maintenance activities (e.g., authorized repair centers).

iii. Cybersecurity considerations of the maintenance process (e.g., how customer data unrelated to the maintenance process remains confidential even from maintainers).

f. The secure system lifecycle policies and processes associated with the IoT product, **including**:

i. Steps taken during development to ensure the IoT product and its product components are free of any known, exploitable vulnerabilities.

ii. The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.

iii. Any post end-of-support considerations, such as the discovery of a vulnerability which would significantly impact the security, privacy, or safety of customers who continue to use the IoT product and its product components.

g. The vulnerability management policies and processes associated with the IoT product, **including**:

i. Methods of receiving reports of vulnerabilities (see Information and Query Reception below).

ii. Processes for recording reported vulnerabilities.

iii. Policy for responding to reported vulnerabilities, including the process of coordinating vulnerability response activities among component suppliers and third-party vendors.

iv. Policy for disclosing reported vulnerabilities.

v. Processes for receiving notification from component suppliers and third-party vendors about any change in the status of their supplied components, such as end of production, end of support, deprecated status (e.g., the product is no longer recommended for use), or known insecurities.

Cybersecurity utility: Generating, capturing, and storing important information about the IoT product and its development (e.g., assessment of the IoT product and development practices used to create and maintain it) can help inform the IoT product developer regarding the product's actual cybersecurity posture.

Information and Query Reception: The ability of the IoT product developer to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.

- The IoT product developer can receive information related to the cybersecurity of the IoT product and its product components and can respond to queries related to cybersecurity of the IoT product and its product components from customers and others, **including**:
    a. The ability of the IoT product developer to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from customers and others in the IoT product ecosystem (e.g., repair technician acting on behalf of the customer).
    b. The ability of the IoT product developer to receive queries from and respond to customers and others in the IoT product ecosystem about the cybersecurity of the IoT product and its components.

Cybersecurity utility: As IoT products are used by customers, those customers may have questions or reports of issues that can help improve the cybersecurity of the IoT product over time.

Information Dissemination: The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.

- The IoT product developer can broadcast to many/all entities via a channel (e.g., a post on a public channel) to alert the public and customers of the IoT product about cybersecurity relevant information and events throughout the support lifecycle. **At a minimum, this information shall include**:
    a. Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.

b. End of term of support or functionality for the IoT product.
c. Needed maintenance operations.
d. New IoT device vulnerabilities, associated details, and mitigation actions needed from the customer.
e. Breach discovery related to an IoT product and its product components used by the customers, associated details, and mitigation actions needed from the customer (if any).

- The IoT product developer can distribute information relevant to cybersecurity of the IoT product and its product components to alert appropriate ecosystem entities (e.g., common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information, *for example*:
  a. Applicable documentation captured during the design and development of the IoT product and its product components.
  b. Cybersecurity and vulnerability alerts and information about resolution of any vulnerability.
  c. An overview of the information security practices and safeguards used by the IoT product developer.
  d. Accreditation, certification, and/or evaluation results for the IoT product developer's cybersecurity-related practices.
  e. A risk assessment report or summary for the IoT product developer's business environment risk posture.

Cybersecurity utility: As the IoT product, its components, threats, and mitigations change, customers will need to be informed about how to securely use the IoT product.

Product Education and Awareness: The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related

information (e.g., considerations, features) related to the IoT product and its product components.

- The IoT product developer creates awareness and provides education targeted at customers about information relevant to cybersecurity of the IoT product and its product components, **including**:
    a. The presence and use of IoT product cybersecurity capabilities, including at a minimum:
        i. How to change configuration settings and the cybersecurity implications of changing settings, if any.
        ii. How to configure and use access control functionality (e.g., set and change passwords).
        iii. How software updates are applied and any instructions necessary for the customer on how to use software update functionality.
        iv. How to manage device data including creation, update, and deletion of data on the IoT product.
    b. How to maintain the IoT product and its product components during its lifetime, including after the period of security support (e.g., delivery of software updates and patches) from the IoT product developer.
    c. How an IoT product and its product components can be securely re-provisioned or disposed of.
    d. Vulnerability management options (e.g., configuration and patch management and anti-malware) available for the IoT product or its product components that could be used by customers.
    e. Additional information customers can use to make informed purchasing decisions about the security of the IoT product (e.g., the duration and scope of product support via software upgrades and patches).

Cybersecurity utility: Customers will need to be informed about how to securely use the device to lead to the best cybersecurity outcomes for the customers and the consumer IoT product marketplace.

Procedural Matters

Initial Paperwork Reduction Act of 1995 Analysis

This document seeks comment on potential new or revised proposed information collection requirements. Therefore, the Commission seeks comment on potential new or revised collections subject to the Paperwork Reduction Act of 1995. If the Commission adopts any new or revised final information collection requirements when the final rules are adopted, the Commission will publish a notice in the Federal Register inviting further comments from the public on the final information collection requirements, as required by the Paperwork Reduction Act of 1995, Public Law 104-13 (44 U.S.C. 3501-3520). The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public to comment on the information collection requirements contained in this document, as required by the PRA. Public and agency comments on the PRA proposed information collection requirements are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].** Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology; and (e) way to further reduce the information collection burden on small business concerns with fewer than 25 employees. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Pub. L. 107-198, see 44 U.S.C. 3506(c)(4), the Commission seeks specific comment on how it might "further reduce the information collection burden for small business concerns with fewer than 25

employees."

Initial Regulatory Flexibility Analysis

71. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the document. The IRFA is set forth in Appendix B of the document. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the document, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the document and IRFA (or summaries thereof) will be published in the Federal Register.

A. Need for, and Objectives of, the Proposed Rules

72. The document proposes a voluntary cybersecurity labeling program for the Internet of Things (IoT) to improve consumer confidence and understanding of security for IoT devices and/or products. Such IoT devices and products are susceptible to a wide range of security vulnerabilities, which can be exploited by attackers to gain unauthorized access to an IoT device or IoT product and its data. Accordingly, providing consumers with a label certifying that an IoT device and/or product satisfies certain baseline cybersecurity standards and has specific cybersecurity capabilities allows a consumer to understand the relative security risk that an IoT device and/or product may pose when making a purchase. The document seeks comments on the scope of the proposed cybersecurity labeling program, including comments on proposed definitions of an IoT device and an IoT product. It also seeks comments on specific technical criteria for the cybersecurity labeling program, including whether other criteria in addition to the IoT Criteria developed by the National Institute of Standards and Technology (NIST), should be considered, and whether and how to develop administrable standards. Finally, the document invites comments on how to administer the cybersecurity labeling program, the appropriate means to fund the costs of running the program, and what program auditing, enforcement,

disqualification and certification revocation processes and procedures should be put in place to ensure that the labeling program is a trusted and valuable resource that consumers can reply upon to assess the security of the IoT devices and/or products that exhibit the label.

B. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

73. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the proposed rules and policies, if adopted. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning has the term "small business concern" under the Small Business Act. A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

74. Small Businesses, Small Organizations, and Small Governmental Jurisdictions. The Commission's actions, over time, may affect small entities that are not easily categorized at present. The Commission therefore describes here, at the outset, three broad groups of small entities that could be directly affected herein. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 30.7 million businesses.

75. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field." The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations. Nationwide, for tax year

2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.

76. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand." U.S. Census Bureau data from the 2017 Census of Governments indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number there were 36,931 general purpose governments (county, municipal and town or township) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts with enrollment populations of less than 50,000. Accordingly, based on the 2017 U.S. Census of Governments data, the Commission estimates that at least 48,971 entities fall into the category of "small governmental jurisdictions."

77. Radio Frequency Equipment Manufacturers (RF Manufacturers). There are several analogous industries with an SBA small business size standard that are applicable to RF Manufacturers. These industries are Fixed Microwave Services, Other Communications Equipment Manufacturing, Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. A description of these industries and the SBA small business size standards are detailed below.

78. Fixed Microwave Services. Fixed microwave services include common carrier, private-operational fixed, and broadcast auxiliary radio services. They also include the Upper Microwave Flexible Use Service (UMFUS), Millimeter Wave Service (70/80/90 GHz), Local Multipoint Distribution Service (LMDS), the Digital Electronic Message Service (DEMS), 24 GHz Service, Multiple Address Systems (MAS), and Multichannel Video Distribution and Data Service (MVDDS), where in some bands licensees can choose between common carrier and non-common carrier status. Wireless Telecommunications Carriers (*except* Satellite) is the closest

industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus, under the SBA size standard, the Commission estimates that a majority of fixed microwave service licensees can be considered small.

79. The Commission's small business size standards with respect to fixed microwave services involve eligibility for bidding credits and installment payments in the auction of licenses for the various frequency bands included in fixed microwave services. When bidding credits are adopted for the auction of licenses in fixed microwave services frequency bands, such credits may be available to several types of small businesses based average gross revenues (small, very small and entrepreneur) pursuant to the competitive bidding rules adopted in conjunction with the requirements for the auction and/or as identified in Part 101 of the Commission's rules for the specific fixed microwave services frequency bands.

80. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time the Commission is not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

81. Other Communications Equipment Manufacturing. This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment). Examples of such manufacturing include fire detection and alarm systems

manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing. The SBA small business size standard for this industry classifies firms having 750 or fewer employees as small. For this industry, U.S. Census Bureau data for 2017 shows that 321 firms operated for the entire year. Of that number, 310 firms operated with fewer than 250 employees. Based on this data, the Commission concludes that the majority of Other Communications Equipment Manufacturers are small.

82. Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment. Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment. This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment). Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing. The SBA small business size standard for this industry classifies firms having 750 or fewer employees as small. For this industry, U.S. Census Bureau data for 2017 shows that 321 firms operated for the entire year. Of that number, 310 firms operated with fewer than 250 employees. Based on this data, the Commission concludes that the majority of Other Communications Equipment Manufacturers are small.

C. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

83. The voluntary cybersecurity labeling program for IoT devices and/or products to provide consumers with accessible information on the relative security of these IoT devices and/or products that the Commission proposes in the document may impose new reporting,

recordkeeping, notice or other compliance requirements on small entities that choose to participate in the program. The requirements may include application or other conformance reporting, licensing, certification and/or other reporting obligations.

84. The proposals in the document build upon other actions the Commission has taken to protect and secure public safety. Accordingly, the proposals being made in this document may require additional analysis and mitigation activities by small and other IoT manufacturers in order to satisfy certain technical criteria or standards for the ability to display an IoT cybersecurity label. At this time, the Commission is not in a position to determine whether the requirements that may be adopted for participants in the proposed cybersecurity labeling program will require small entities to hire professionals in order to comply and cannot quantify the cost of compliance with the potential requirements and obligations that may result in this proceeding. Among other things considered, the Commission inquires about the options for it to address the costs of running and administering the labeling program including whether there may be application fees charged by third-parties administering the program and whether there is oversight the Commission should exercise over such charges. The Commission seeks comment on these issues and anticipate that the information it receives in comments will address these matters and any broader cost issues for small entities that may choose to participate in the proposed labeling program.

85. In light of the importance of mark integrity and the need to build consumer confidence and trust in the security of IoT devices and products that will display the Commission's IoT label, regardless of the size of the entity seeking to participate in the proposed cybersecurity labeling program, adherence by all participants to the same Commission rules is necessary. However, the Commission expects that the comments it receives will help it identify and evaluate relevant matters for small entities before adopting final rules for the labeling program, including any compliance costs and burdens that may result from the proposals and other matters discussed in the document.

D. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

86. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."

87. The Commission's development of a voluntarily cybersecurity labeling program for the IoT products and devices builds on the work of the National Institute of Standards and Technology (NIST) which produced labeling criteria for cybersecurity capabilities of IoT consumer devices. Using the work of NIST as a foundation has the potential to minimize the economic impact on small entities for several reasons. First, NIST took into account existing consumer product labeling programs and information provided by diverse stakeholders. Next, two of the key elements NIST identified for labeling were encouraging innovation, and being practical and not burdensome. Further, the Commission believes building on the approach NIST developed for IoT cybersecurity labeling will provide a level of consistency with the requirements it establishes for the entities subject to Commission regulation that choose to participate in the Commission's cybersecurity IoT labeling program.

88. In the document, the Commission considers and seeks comment on various compliance requirements that it could consider in advancing a voluntary cybersecurity labeling program. More specifically, the Commission considered the NIST definition for IoT devices which defines IoT devices as devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi,

Bluetooth) for interfacing with the digital world, and determined that it should propose an alternative definition. The Commission's proposed definition modifies the NIST definition to add "Internet-connected" because a key element of the IoT is the usage of standard Internet protocols for functionality, which exposes IoT devices to the security threats and challenges related to being connected to the Internet. The Commission's proposed definition also includes the requirement that devices must be capable of intentionally emitting radio frequency energy because the relevant scope of Commission's statutory authorities focus on devices that intentionally emit radio frequency energy.

89. Although the Commission includes in its definition devices that intentionally emit radio frequency energy, it considered whether there are unintentional radiators or incidental radiators that should be included in the program, and if so whether the Commission should revise the definition to omit the word "intentional." Alternatively, the Commission inquires if it should consider adding unintentional or incidental radiating devices to the program at a later date. In addition, while the Commission refers to devices and products in the document, it inquires whether it should expand the proposed scope of the cybersecurity labeling program and definition of devices beyond IoT devices to apply to IoT products. Under this expanded alternative the Commission could define an IoT product as an IoT device and any additional product components (e.g., backend, gateway, mobile App) that are necessary to use the IoT device. A further alternative the Commission considered, is whether to limit the IoT labeling program to consumer IoT devices or products intended for personal use, or to include "enterprise" devices or products intended for industrial or business uses and any additional considerations that would need to be accounted for with such devices or products. The Commission seeks comment on these inquiries and alternatives in the document, in addition to comments on the proposed definition.

90. Regarding the content and updating of the IoT label on the physical device, product, or packaging, the Commission believes the simple approach proposed in the document will result in

cost savings which could minimize the impact of these requirements for small entities. The Commission's proposal is to have the physical device, product, or packaging simply indicate that the manufacturer participates in the FCC's labeling program by having the FCC mark along with the related QR Code and/or the URL to the IoT registry. The detailed information on the IoT device or product will be made available on the device or product's webpage within the IoT registry using an QR Code and/or a URL. When the device or product's webpage within the IoT registry is updated to indicate for example, that the device or product's authorization is outdated, and/or the device or product is no longer maintained or updated, using the QR Code and/or the URL provided next to the FCC mark the information can be accessed on the device or product's webpage within the IoT registry. Updating requirements for the device or product's webpage within the IoT registry could alleviate the need for the Commission to adopt additional notification requirements which would increase costs for small entities.

91. The Commission also considered and seeks comment on alternatives on how to address the end-of-life issues for devices previously receiving authorization under the program. For example, the Commission considered whether the label should include the specific date, or the year the authorization was awarded, or an expiration date. Further, the Commission considered whether it would be sufficient to provide consumers with additional information via the QR Code regarding the current security status of a device, and whether the QR Code-linked website should indicate when the label was issued by the Commission, and when the information on the webpage last updated.

92. In the area of accessibility, to ensure that any IoT cybersecurity label information the Commission adopts is accessible to persons with disabilities, the Commission considered an alternative that would alleviate the need for the Commission to establish and impose new accessibility requirements on small entities and other participants in the labeling program. Consistent with its approach with broadband consumer labels in 2022, in the document the Commission considered and seeks comment on relying on the existing legal requirements in the

Americans with Disabilities Act (ADA) and following the guidance developed by the Web Accessibility Initiative, which the Consumer Advisory Committee (CAC) determined is the best method to ensure accessibility to printed and online information is made available by providers.

93. Further, rather than proposing rules at this juncture, in the document the Commission seeks comment on costs associated with the proposed cybersecurity IoT labeling program, and on investigation, disqualification and enforcement processes to maintain the integrity of the devices or products that will be labeled under the program. The Commission's actions on all of these matters have the potential to minimize the impact of the cybersecurity IoT labeling program the Commission adopts on small entities.

94. Regarding investigation, disqualification and enforcement, as discussed in the document, the Commission considered and seeks comment on whether to have random audits of IoT devices or products to confirm continued compliance; whether the Commission should adopt disqualifications procedures similar to those adopted for the ENERGY STAR program by the Environmental Protection Agency (EPA); what additional non-compliance or disqualification measures would be appropriate in addition to authorization revocation, and whether there should be an appeal process available to applicants that are denied authority to use the IoT label. Additionally, the Commission seeks comment on what recordkeeping and audit requirements could be adopted for purposes of compliance review.

95. The Commission expects to more fully consider the economic impact and alternatives for small entities following the review of comments filed in response to the document. Having input from interested parties will allow the Commission to better evaluate options and alternatives to minimize any significant economic impact on small entities that may result from the proposed cybersecurity IoT labeling program and the inquiries and alternatives discussed in the document. The Commission's evaluation of this information will shape the final alternatives it considers to minimize any significant economic impact that may occur on small entities, the final conclusions it reaches and any final rules it promulgates in this proceeding.

E. Legal Basis

96. The proposed action is taken under authority found in sections 1, 2, 4(i), 4(n), 301, 302, 303(b), 312, 333, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(n), 301, 302a, 303(b), 312, 333, 503; and the IoT Cybersecurity Improvement Act of 2020, 15 U.S.C. 278g-3a to 278g-3e.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

97. None.

FEDERAL COMMUNICATIONS COMMISSION

Katura Jackson,
Federal Register Liaison Officer.
[FR Doc. 2023-18357 Filed: 8/24/2023 8:45 am; Publication Date: 8/25/2023]